

STATEMENT OF
REAR ADMIRAL GEORGE N. NACCARA
ON THE Y2K READINESS OF THE
UNITED STATES COAST GUARD
BEFORE THE
COMMITTEE ON TECHNOLOGY AND INFRASTRUCTURE OF THE
UNITED STATES HOUSE OF REPRESENTATIVES

Good morning, Mr. Chairman and distinguished members of the committee. I am Rear Admiral George Naccara, the Coast Guard Chief Information Officer. I have responsibility for the Coast Guard's Y2K project. I want to thank you for giving me the opportunity to testify before you today.

Today I want to address four major aspects of the Coast Guard Y2K project. They are repair of our own systems, our contingency planning initiatives, our outreach to the maritime industry and boating public, and the cost of all of these efforts to the Coast Guard.

The Coast Guard is keenly aware of the potential for disruption posed by the so-called millennium bug, both in Coast Guard readiness, as well as in the maritime economy. In fact, the Coast Guard experienced a Y2K disruption in early 1997. We had a failure in a software program at the Coast Guard Institute in Oklahoma City. The program triggers

Droundy/public/Senate Special Committee on the Year 2000

mailing to all correspondence course enrollees of an end of course test with a three-year completion window. In January 1997 the three year window suddenly fell beyond the start of the new millennium, and the program, unable to correctly interpret the “00” end date of the year 2000 malfunctioned, and in so doing deleted hundreds of student records. The staff at the Institute required two weeks to correct the problem. It was a sobering wake up call. Our industry partners have learned similar lessons. One major shipper told of spending thousands of dollars to identify and replace systems on their ships potentially affected by the Y2K problem, only to experience a subsequent Y2K failure on one ship after an on board power loss. Those that have had these experiences are very focused on timely repair of their systems, as well as preparing for all contingencies.

The Coast Guard Y2K Program

We are engaged on two major fronts in dealing with this serious international concern. First, we are working diligently to ensure our own information technology is ready for the millennium. Our motto is “Semper Paratus” – Always Ready, and in consonance with that, we want to ensure that we can continue to deliver our marine safety, environmental protection, search and rescue and maritime law enforcement services to the public without interruption. On that score I am pleased to report that we are making good progress, and we expect our boats, ships and planes will be ready and operating on 1 January 2000, and thereafter, as they always have been, with minimal disruption. In addition, our managers and technical staffs are repairing the administrative and support systems that underpin our

operations, and we expect them to be repaired and working when the new millennium dawns.

Let me give you the specifics. As you can imagine, in 190 aircraft, 225 Cutters, thousands of small boats, and 15,000 facilities of all sizes nationwide, the Coast Guard, though small compared to its counterparts in the Department of Defense, has a sizable inventory of computer systems, software applications, and electronic equipment. The list includes large operational systems like the Automated Mutual assistance Vessel Rescue System (AMVER) and the Marine Safety Information System (MSIS), large personnel and financial systems like our pay and personnel system (PMIS/Jumps) and Large Unit Financial System (LUFS), and other equipment like telephone switches and radio consoles. Of our total inventory of systems, we report 75 as mission critical to the Office of Management and Budget (OMB). As of 30 September, we have renovated approximately 90% of the 75 systems, and expect to complete the renovation, testing, and implementation phases on these by March 31, 1999, the OMB completion date. A couple of systems, the Finance Center Information Resource and Management System or FIRMS, and the Aviation Maintenance Management Information System (AMMIS) have fallen behind the OMB milestones for renovation, but we expect to have these systems renovated, tested, and implemented as well by the end of March 1999. Though we are very concerned about the delay in completing renovation work on these systems, we remain confident that they will be implemented by the final OMB milestone of March 31, 1999. We have just learned that the core system of the Vessel Traffic Management Service (VTS) in Valdez, Alaska cannot be repaired, but must be replaced, at a cost of

\$1.2M. Though this represents a previously unanticipated additional cost, it will provide us by summer 1999 with a reliable system with which to manage ship traffic in Prince William Sound. All told, I believe I can say with confidence that all Coast Guard mission critical systems will be ready well before the dawn of the millennium.

In addition, we have asked program sponsors to pay special attention to other systems which, though they may not be on the mission critical list, support our Coast Guard personnel, such as medical or training systems. We want our members and their families to suffer minimal disruption. We will need them focused on other problems when the millennium dawns.

On the operational front, we are taking a fresh look at our ships and airframes as integrated operational systems, and undertaking steps to ensure that the platforms en toto are ready. During 1999, we expect to participate with the Navy in operational evaluations of these platforms as part of field exercises intended to validate our readiness. For example, as you may be aware the Chairman of the Joint Chiefs of Staff has canceled the major annual joint service exercise "Positive Force" for 1999. In its place, the Services will play "Positive Response Y2K," with a focus on the Y2K readiness of participating services' operational assets. I anticipate the Coast Guard will be approached to participate in other related activities during 1999, which my staff likes to call "the year of the contingency plan." The Coast Guard will leave no stone unturned to prepare its technology for the millennium, but will also be ready to continue responding to the call

even if a piece of technology lets us down. We will be “Semper Paratus,” as our motto states.

Contingency and Continuity of Operations Planning

Despite the feverish pace of repair work inside and outside the Coast Guard, two things are certain. One is that not all government, business, or industry systems will be repaired in time. On that score, the Coast Guard may be more fortunate than others within the federal government, as the scope of our repairs is manageable. By the end of 1999 we can expect to complete repairs not only to all of our mission critical systems, but also to most other systems that may not have been designated mission critical, but are important to our operations. The second certainty is that errors will surface in repaired systems, both during testing and then during actual operations. Independent testing contractors have found error rates from 2 to 10% in systems that have been repaired **and tested** by their owners. For this reason, the Office of Management and Budget prudently requires that all systems have workable contingency plans in place in the event of system failure. Though our focus as a Service has been on the 75 mission critical systems, we have directed our unit commanders and headquarters program managers to prepare contingency plans for all systems that are important to the functioning of their units.

To prepare on a national level, the Coast Guard has launched a continuity of operations initiative called Operation Millennium Approach/Millennium Dawn. We recognize that

even if Coast Guard systems and equipment are prepared for the year 2000 rollover, there is the potential for failures across the country, in public infrastructure, among our suppliers and business partners, and in the industry we regulate. To properly prepare for external disruptions that may impact the Coast Guard, we are convening a planning meeting in St. Louis on October 8, 1998 to be attended by Area and District Chiefs of Staff. They will inventory and evaluate the range of possible Y2K impacts upon the Coast Guard from region to region, determine the Service-wide, Incident Command System (ICS) based organization needed to be fully prepared to respond to disruptions while continuing operations, and issue planning guidance for Coast Guard wide use. By mid-1999, the team will issue an Operations Order for Operation Millennium Dawn, which will spell out actions to be taken across the country by all levels of the organization. In addition, as efforts ramp up to prepare a coordinated federal level response organization with agencies such as the Federal Emergency Management Agency and state and local Emergency Operating Centers, we will be configured to establish liaison points and interact seamlessly with such a federal level organization.

I should point out that since Y2K is a global phenomenon, it is possible that a Y2K-ready Coast Guard could be called upon to assist others who have failures, including other U. S. government agencies, maritime industry and boating public partners, even other governments in the hemisphere. Our Y2K readiness could carry us beyond our shores.

Outreach

The second major focus of our program is our outreach efforts to help ensure the success of our partners and customers in the marine industry in dealing with their Y2K problem.

The United States economy is extraordinarily dependent upon maritime shipping. I only need to mention that according to the Energy Information Administration, more than 50% of the oil consumed in this country comes to us from foreign sources through our ports.

Add to this the fact that, according to statistics kept by the Maritime Administration, 95% of all the cargo entering the U. S. comes via our ports, and over 97% of that comes in foreign ships. Any disruption of the cargo and especially oil flow, for even a few days, would have a discernable effect on our economy, particularly during the winter heating season.

We are anxious to ensure that the ships, and the ports, are ready. In consonance with the call of Mr. John Koskinen, Chairman of the President's Council on the Year 2000

Conversion, to build Y2K awareness with our partners in the maritime industry, we have mounted several outreach initiatives. At my direction, regional Y2K awareness

conferences have been scheduled for this fall and early winter on the East, West, and Gulf Coasts, as well as in the Great Lakes region and on the Inland Rivers. Over a thousand representatives of maritime companies will attend these conferences to learn more about what their counterparts are doing, and to share best practices in Y2K project management.

We have created a Y2K awareness brochure that is being distributed by 46 Captain of the Port offices around the country. They will be distributed to the masters of vessels, both foreign and U.S. that we board during routine inspections, to facilities operators and cargo transfer terminals and to participants at local industry days hosted by our Captains of the

Port. They will also be distributed by thousands of our Coast Guard auxiliarists at boating safety courses, courtesy marine examinations, and boat shows to the recreational boating public. We have put information about Y2K on our web sites, and information on the Global Positioning System rollover issue is being broadcast by our Navigation Information Center. We published a notice on the Y2K problem and the marine industry in the Federal Register, and on the international scene, we succeeded in persuading the Maritime Safety Committee of the International Maritime Organization to publish a circular on the Y2K issue. We will continue these efforts into 1999, with an increased emphasis on the importance of contingency planning. We are considering a requirement for contingency plans at the port level. We are also encouraging existing maritime associations and port safety committees to establish Y2K readiness planning groups, and to establish port readiness web sites to disseminate information on the status on Y2K issues in the port and how they are being addressed.

It is worthwhile to note, in connection with outreach, that the Coast Guard has elected to stress aggressive Y2K education and awareness building in its approach to the maritime industry. We plan no additional regulatory actions related to Y2K, for two reasons. One is that we can work cooperatively with industry, capitalizing on the powerful economic incentives they have to avoid delay, to ensure they prepare their technology for the millennium. Secondly, we already have the regulatory authority we need to ensure safety in our ports and on board vessels, and will exercise it as we have in the past to ensure vessels are safe and seaworthy. We are putting the word out that ships which have problems may be restricted in their movements based on the criticality of the ship's system

that is inoperative and its effect on the ability of the vessel to proceed safely. The root cause of the system problem may be related to Y2K; if this is the case, the ship will have to demonstrate that this error has been corrected before the restrictions will be lifted. For example, if a vessel entering port conducts the required steering test and detects a problem, regardless of cause, it must be reported immediately to the Coast Guard Captain of the Port who will take appropriate action to control the movement of the vessel in light of the steering problems. If the cause of the system malfunction is Y2K related, that problem must be corrected before the ship may proceed on its way unrestricted. As stated, the shipping company is motivated by economic incentives to correct problems, and get their vessel back into service.

I would like to say that our port evaluations to date indicate no major problem in this regard. Most larger companies take the Y2K problem very seriously, and have active projects in place to deal with it. Some smaller companies may have come to awareness more slowly, but I recall the representative of a small tug and barge company who spoke at our conference in Hampton Roads last month. Once alerted to the seriousness of the problem, the company moved promptly to replace affected systems.

The Cost of the Y2K Efforts

Needless to say, the repair, contingency planning, and outreach efforts we have undertaken have brought with them ever mounting costs. The estimate for overall Coast Guard costs stands today at \$34M, of which \$21M was included in the DOT request for

supplemental FY 1999 funding from the Congress. I am very aware that as we prepare to participate in major Y2K-related operational exercises, hire contractors, expand our staff, broaden our outreach to industry both domestically and internationally, and travel to and/or present more conferences, those costs could double or even triple. We are willing and even eager to carry out these activities, but we do not have the funding in our budget to support them. I hope that the committee will work with us in doing all that can be done to make sure the Coast Guard, the maritime industry, and the U. S. economy are not significantly disrupted by the Y2K problem starting a little less than a year from now.

I will be happy now to answer any questions you might have.